

Online report sponsored by:



BROCADE

Mainstreaming Cloud Computing

Inside

Cloud computing almost routine	s2
Agencies flee public clouds	s5
SaaS remains the biggest cloud	s7
Security still a hurdle	s9
Lukewarm views of FedRAMP	s11



Cloud computing almost routine

Nearly four out of 10 survey respondents have embraced some form of cloud architecture

Cloud computing is a novelty no more in government IT departments. It has quickly matured to the point where it is on the threshold of becoming a mainstream source of technology for military and civilian agencies and state and local governments.

And as government agencies and departments have learned more about cloud computing, they have gained a more mature perspective on the benefits and risks associated with cloud computing.

The myriad benefits, as well as various mandates, have increased cloud computing deployments to the point that nearly four out of 10 respondents has either adopted cloud computing or are in the process of adopting the architectures for at least some applications or processes, according to a January 2012 survey of almost 300 respondents by the 1105 Government Information Group. A year earlier, only a quarter of the respondents were using or implementing cloud computing.

The federal government's cloud-first policy, first discussed in the 2010 Federal Cloud Computing Strategy, is among the many mandates driving agency consideration

and adoption of the architecture. Cloud first requires federal agencies to consider a cloud option first with every technology project. It stipulates trying to use commercial cloud technologies where feasible and only subsequently considering private government clouds.

However, federal, state and local agency respondents to the survey indicated quite strongly that such mandates are in conflict with security concerns. Indeed, more than half indicated that cloud solutions aren't secure enough for their agencies — a proportion that hasn't changed despite a year of intense examination, testing and deployment of cloud computing.

That tug-of-war — the need to comply with various mandates or the expected cost savings while dealing with security worries — is what may be driving agencies to turn to software as a service (SaaS) as a way to get comfortable with the cloud model without incurring too many security risks, said Renell Dixon, a managing director of the public-sector practice at global professional services firm PricewaterhouseCoopers.

“Moving from managing a traditional software package in their own environment to accessing it in the cloud is a relatively low risk way of gaining the benefits of cloud — reducing an agency's carbon footprint and reducing costs associated with operation and maintenance,” Dixon said. “These lower risk options are a popular way for government agencies to dip their toe in the water and learn as they go.”

While SaaS is the most popular form of cloud computing in federal government, the survey found that agencies also are using infrastructure as a service (IaaS) and platform as a service (PaaS) as cloud delivery mechanisms. The survey also found that backup, storage, compute services and collaboration are the most popular IT functions currently being delivered by some type of cloud service.

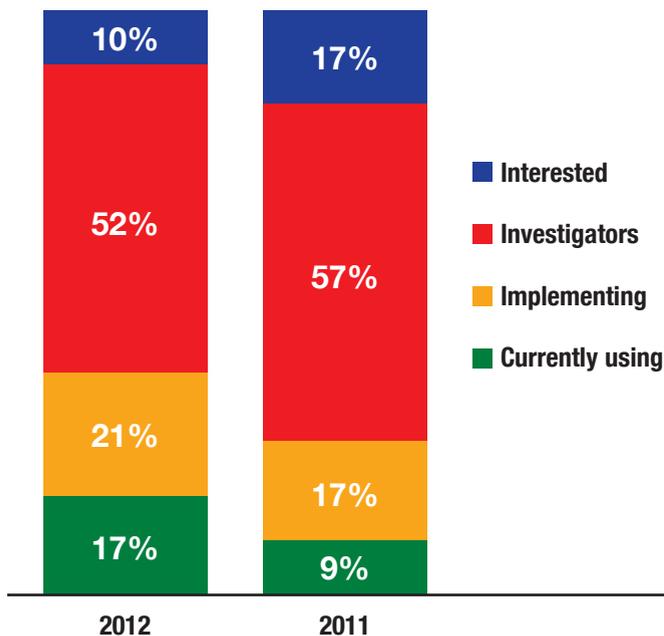
Disappointing savings

The survey also found that while cost savings have been significant, most respondents report that the savings have been somewhat less than anticipated. Of the four basic types of clouds — public, private, community and hybrid — respondents found private clouds to be the most cost-effective.

While two-thirds of the respondents had expected cost savings from a switch to cloud computing, half said they had saved less. A third achieved the savings they expected and 15 percent achieved more savings than expected.

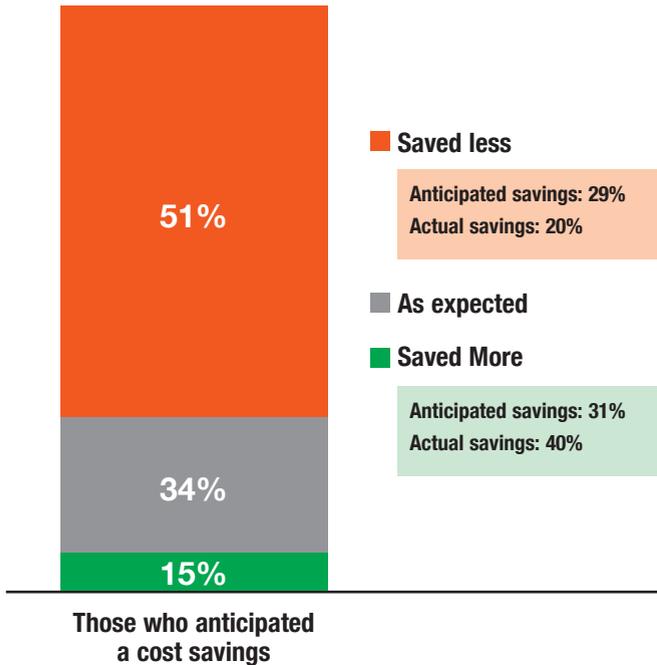
CLOUD ADOPTION GROWING

Phase of adoption by % of respondents



HALF SAVED LESS THAN EXPECTED

% of respondents who indicated cost savings



Specifically, the expected savings were about 30 percent, but a significant number of organizations had actual savings of only 20 percent. A few agencies had pleasant surprises, though — their actual savings were 40 percent.

The biggest unpleasant surprise in the cost reduction initiative was the need for other technology when shifting to the cloud. A host of unanticipated hardware, software and data bills are among the potential culprits, say consultants.

“Federal agencies are faced with transitioning away from antiquated legacy systems to the cloud, which for some requires an overhaul of servers, storage, network and other types of technology to provide the right foundation for cloud,” explained Deniece Peterson, senior manager of industry analysis at Deltek, a Herndon, Va.-based consultancy and market research group.

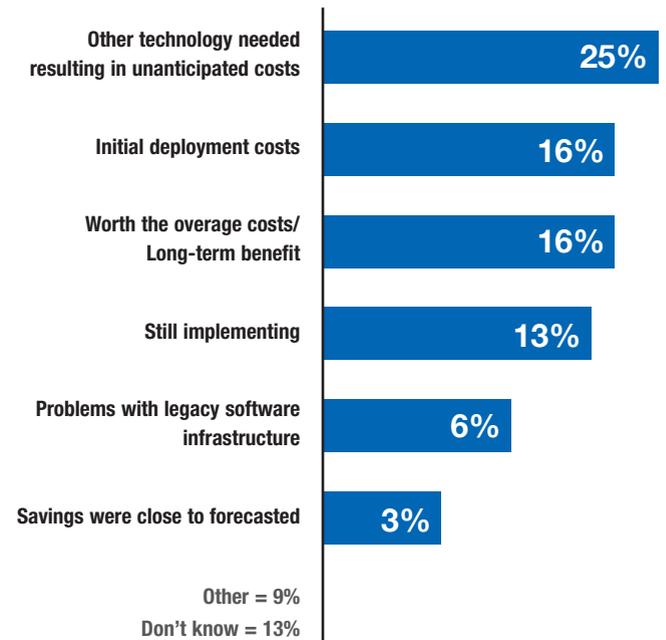
Another example of the learning curve about cloud is the decline in use of the public cloud by government agencies. In one year, the use of the public cloud decreased as a source of infrastructure services to 10 percent, from 23 percent of respondents. Use of the public cloud for platform services also declined, to 8 percent from 17 percent. However, use of the public cloud for software delivery increased to 25 percent from 23 percent.

Decline in public cloud deployments

The public cloud has taken some hits in the press in the form of security breaches and denial-of-service attacks, which may have shaken agencies’ confidence and accounted for

UNEXPECTED CLOUD COSTS

Reasons why respondents experienced lower savings than anticipated (multiple selections allowed)



the downturn in public cloud use in the government. That may be why the survey found that the use of private clouds increased to 68 percent from 43 percent for IaaS while increasing to 63 percent from 55 percent for PaaS.

Other viable cloud architectures offer security and cost saving possibilities. One is the hybrid cloud — a combination of public and private clouds that puts more sensitive data out of reach to the public while putting less sensitive data in a public cloud. This type of scenario not only helps satisfy various mandates but also can increase cost savings rather than putting the entire infrastructure or platform into a private cloud.

“When the cloud initiative was first announced, there was a lot of interest in the public cloud because the mantra was to save money. Now what’s happened is that people have found that the public cloud does save money, and they are looking to extend it but with an eye on security,” explained Kevin Jackson, general manager for cloud services at NJVC, a Vienna, Va., technology services provider for government, and CIO of GovCloud.com. “That brought them to the idea of the hybrid cloud — a model that is driven by more awareness and understanding of the cloud economic and operational model.”

Another cloud model generating growing interest is the community model, where a cloud infrastructure is shared by several organizations or agencies and supports a specific community, application or platform. For example, several agencies could rely on one billing, HR or email application

or platform in the cloud, with all agencies paying the agency that hosted the offering for the privilege. It's a great way to eliminate duplicate investment and implement best practices such as the requisite level of security.

One of the major drivers for adoption of the community cloud model is Federal CIO Steven VanRoekel's shared-first initiative, which aims to eliminate duplication and leverage technology, procurement and best practices across government. The first target is consolidating data centers, but VanRoekel has made it clear that cloud computing will be a main driver in the shared-first model.

Moving forward

Dixon insists that the combination of education, experience and the advent of the Federal Risk and Authorization Management Program standards — regulations intended to standardize cloud security — will increase cloud adoption in government significantly over the next few years. But

even after FedRAMP becomes operational, cloud providers have two years to become certified as fully compliant, which means that it may take that long for agencies to become fully comfortable with the security aspects of the cloud.

Jackson's advice to agencies is to be patient — security and cost savings will improve with time. And as those benefits and security continue to mature, agencies become more comfortable with the culture changes involved in reliance on the cloud for computing resources.

"I like to compare cloud computing to the idea of opening up a bank in the 1800s in a Western town. People were used to keeping their money under their mattresses, and they don't trust the concept of a bank," Jackson explained. "But over time, a few people use it and others see that it seems to be safe. People begin to trust the concept and get more comfortable with it. Cloud is like that. Cloud providers have to build trust with their customers, and the currency is information." ●

Survey methodology and demographics

In January, an independent survey and research organization commissioned by the 1105 Government Information Group sent an email questionnaire to readers of the group's various publications and websites, including *Federal Computer Week*, *Government Computer News*, *Washington Technology*, *Federal Daily* and *Defense Systems*. The responses were filtered to include only officials of government agencies who were involved in IT decisions and interested in cloud computing.

Of the 289 validated responses, roughly one-third are from civilian agencies of the U.S. government, another third are from various defense-related agencies and the other third are from state or local government agencies.

More than three quarters of the respondents identified themselves as technical decision-makers — they are engineers, technicians, and project or program managers. The remainder are agency executives or operational managers.



Agencies flee public clouds

Security concerns leave agencies wary about using a public cloud

Forget all the buzz about the public cloud — that’s yesterday’s news.

Public cloud use by government agencies plummeted in 2011 as the source of infrastructure or platform services, according to a January 2012 survey of almost 300 government officials by the 1105 Government Information Group.

Just 10 percent of respondents who have already adopted cloud computing are using a public cloud for infrastructure as a service (IaaS), down from 23 percent last year. Platform as a service (PaaS) declined to 8 percent of respondents from the 17 percent in 2011.

Use of the public cloud for software as a service (SaaS) in 2012 increased slightly, up 2 percent to 25 percent of respondents.

For the vast majority of agency respondents who have dropped public cloud computing as a source of IT resources, the major concern is security. Survey participants rated public clouds as less secure than any other cloud computing model.

Major security breaches by large public cloud users, including an attack on Google’s password system in 2010 and a major security breach involving about 60 million email addresses from marketing service firm Epsilon in 2011, certainly didn’t help perceptions, said Renell Dixon,

managing director of PricewaterhouseCoopers’ federal practice.

“The negative press about the public cloud may have created a scare, and it’s up to both government and public cloud providers to educate potential users about the security of the public cloud,” she said. “Government is doing a good job, but cloud providers have to do a better job showing how they as an industry are addressing security and how they will self-govern.”

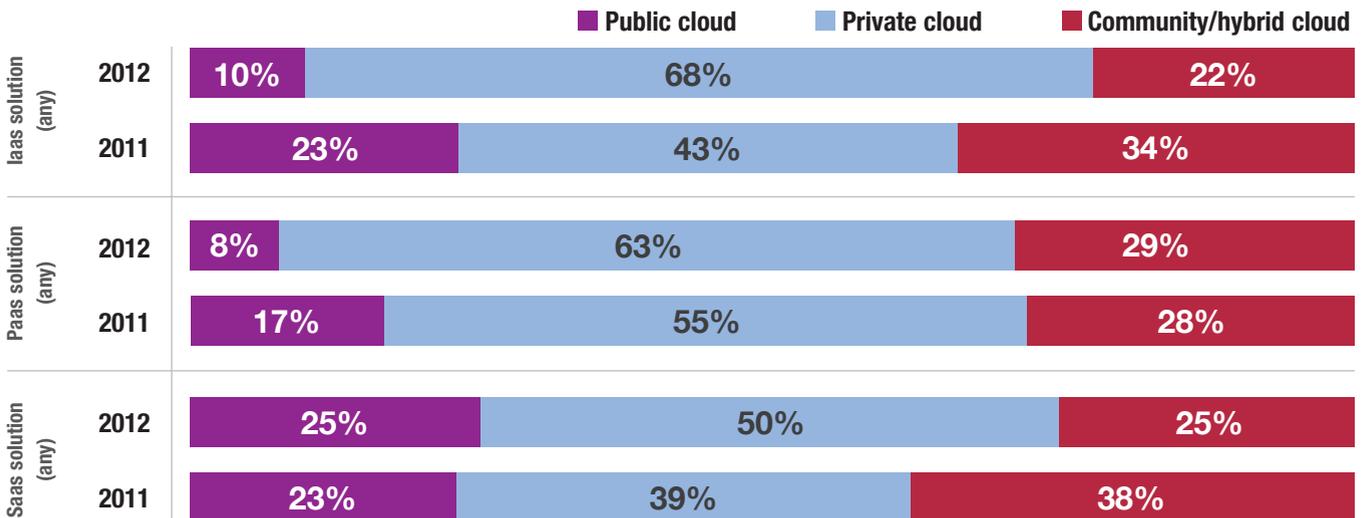
The dip in the use of public clouds is a natural progression of cloud computing in the government, said Deniece Peterson, senior manager of federal industry analysis at Deltek, a Herndon, Va.-based consultancy and market research group.

“There have been a lot of lessons learned over time,” she said. “As agencies gained more experience, got more comfortable and had more information, they became better able to determine the best approach.”

One way to get more comfortable with the public cloud is by dipping a toe in the water, Peterson says. That means potentially adopting some sort of hybrid model, where sensitive information is cordoned off in a private area of the cloud and less sensitive data can take advantage of the cost benefits of the public cloud. The sharp shift to the private cloud among survey respondents indicates some support for

PUBLIC CLOUD SHRINKING

% of respondents using a public, private or hybrid architecture





this approach — private cloud versions of IaaS, PaaS and SaaS increased dramatically in 2012.

One way of arranging the hybrid approach is by using a public cloud provider but having it host your infrastructure or platform in a closed-off area, according to consultants. For example, if an agency is consolidating 20 data centers to one cloud-based data center, the public cloud provider might host a cloud just for that agency.

Another option is asking a public cloud vendor to build

a government cloud just for them. “That way, the vendor takes on the cost of building it, but then they get the benefit of managing it and getting longer-term revenue,” Peterson notes. At the same time, the agency will have fewer security concerns.”

While the community and hybrid cloud approaches are declining in favor among survey respondents, consultants say they are worth a second look. ●

SaaS remains the biggest cloud

Software as a service (SaaS) — accessing software applications in the cloud instead of hosting them on-premises — remains the most popular form of cloud computing used by federal, state and local government agencies. However, interest in platform as a service (PaaS) and infrastructure as a service (IaaS) are growing faster, according to a January 2012 survey of government IT officials by the 1105 Government Information Group.

Roughly one-quarter of respondents use some form of SaaS compared to 19 percent using IaaS and 16 percent using PaaS. And even larger numbers of respondents are considering types of cloud computing, especially SaaS and IaaS.

“SaaS has been the strongest cloud category in government since the beginning, and for good reason. You can use your existing infrastructure and sign up for an application in the cloud, and it’s easy to switch on and get started,” said Kyra Kozemchak, a senior research analyst at Deltek, of Herndon, Va., which sells software and services, such as research on government IT patterns.

The 1105 Government Information Group survey found that although all areas of SaaS are generating interest, some are more widely adopted than others. The most popular SaaS functions are:

- Collaboration;
- Content and document management; and,
- Customer resource management.

SaaS applications for billing, health and wellness, human resources and enterprise resource planning were among the least used applications in government, probably because of the sensitive nature of the data. The survey found that SaaS was most commonly implemented in a private cloud environment.

While only 19 percent of respondents use IaaS — a model in which an organization uses computing equipment in the cloud to run their internal processes — that number is up from just 9 percent last year. The most popular uses of IaaS by federal agencies include backup and storage, recovery, and compute cycles.

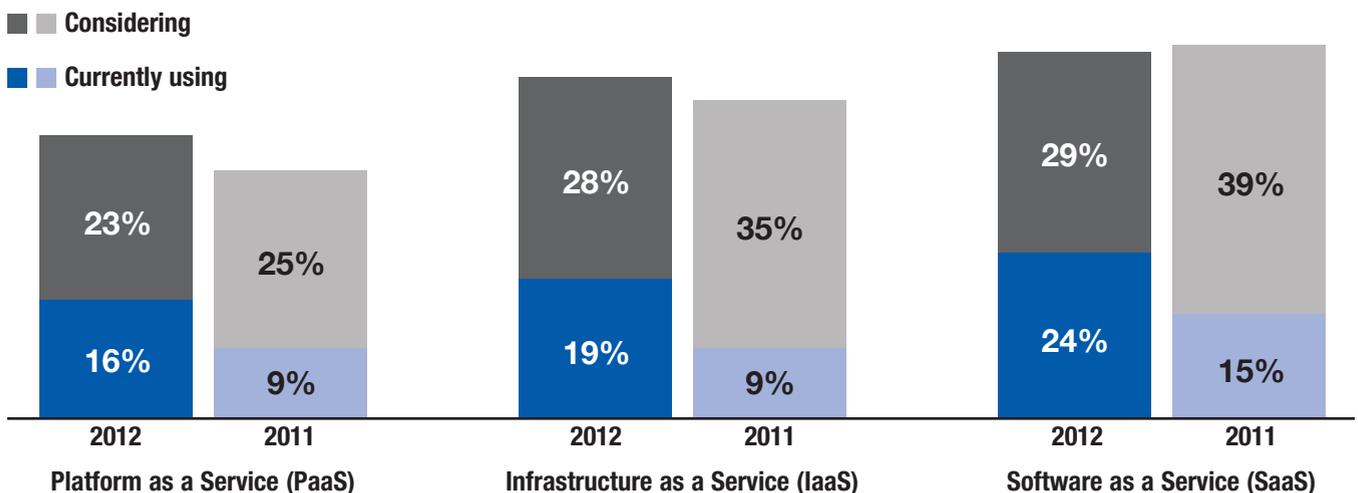
Use and interest in PaaS — the process of relegating an entire platform, including hardware, operating systems, storage and network capacity, to the cloud — shows a similar pattern, with 16 percent using some form of PaaS. That is up from 9 percent a year ago. The most common uses of PaaS by federal agencies are development and testing, database management, and business intelligence.

One of the reasons PaaS and IaaS score lower than SaaS for government agencies is because they are more critical parts of the computing paradigm. Many IT decision-makers aren’t quite ready to turn that part of their IT foundation over to the cloud. That’s partly because of security concerns and the culture that has grown up around infrastructure and platforms in the government, Kozemchak said.

“Even within the government, there is the idea that people own their piece of the pie and, with IaaS in particular, they

OUTLOOK FOR SAAS, IAAS, PAAS

% of respondents who indicated their use or consideration of different types of cloud services





have to give up some of that ownership when they go to the cloud,” she said.

Still, both PaaS and IaaS — not to mention SaaS — are expected to grow. The survey reinforces that claim, finding that within two years, 39 percent want to be using some form of PaaS, 47 percent some form of IaaS, and 53 percent some type of SaaS.

Prompts from the federal government are surely helping those numbers along. On the PaaS side, the National

Institute of Standards and Technology consider PaaS part of the federal Cloud Computing Reference Architecture, and Federal CIO Steven VanRoekel has said that PaaS is an important part of his shared-services initiative. On the IaaS front, the Homeland Security Department’s award of the first task order using the General Services Administration’s IaaS blanket purchase agreement in October 2011 speaks well of the use of IaaS in government over time. ●

Security still a hurdle

Despite advances in cloud security and the efforts of federal government to address the issue through the Federal Risk and Authorization Management Program guidelines, security remains a stumbling block for many agencies when it comes to the cloud.

According to a January 2012 survey by the 1105 Government Information Group, more than half of the respondents indicated that cloud solutions simply aren't secure enough. The majority of respondents mentioned potential data loss or leakage, lack of robust identity authentication and credential management, the inability to clarify ownership of records and data in a cloud environment, lack of secure and timely identity provisioning, and concern that cloud data won't remain within U.S. borders.

Although security is a concern for federal agencies with every type of cloud implementation, the biggest area of government concern by far is security in the public cloud. Survey respondents rated private clouds a 69 on a scale of 1 to 100 for being strongly associated with security and data protection, while they rated the public cloud only a 39.

The survey also found that, despite evidence to the

contrary, a growing majority — 60 percent, versus 54 percent last year — believe cloud computing security risks are greater than on-premises security risks.

“That’s a misconception to some point, but it’s understandable because of some well-publicized security breaches,” said Deniece Peterson, senior manager of federal industry analysis at Herndon, Va.-based Deltek, a software and services provider. “An argument can also be made that public clouds are more secure because it’s the provider’s bread and butter and because their business is running a multi-tenant environment.”

Security concerns should slowly decrease over time, mainly due to the ratification of FedRAMP last December and its operational rollout in the third quarter of this year, said Renell Dixon, managing director at PricewaterhouseCoopers’ public sector practice.

“For a long time, government agencies and cloud providers have been waiting for a framework that could help them understand what they could do to address some of the security concerns around this new environment,” Dixon said. “Now that FedRAMP is a reality, I’ve seen the pace of cloud adoption pick up as well as early adoption of new FedRAMP controls by federal cloud providers. Agencies that were just considering it are now starting to fast-track those decisions because cloud providers are anticipating the need and focusing more on security.”

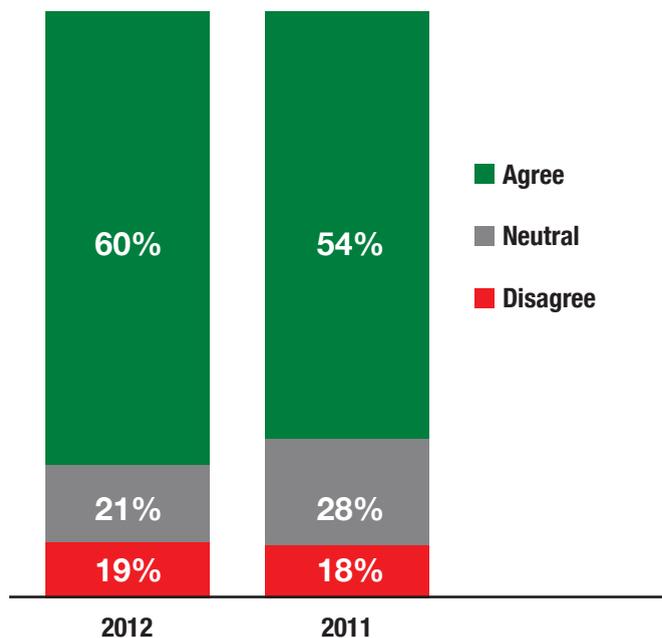
But relying solely on FedRAMP for security assurance in the cloud isn't the only factor agencies should consider. In addition, they should ask a lot of questions of cloud providers on their own, such as how the providers have incorporated audit and assessment tools, as well as continuous monitoring tools and techniques, into their cloud service.

Dixon says federal government decision-makers are leaving nothing to chance when it comes to security.

What the federal government wants to do is pull continuous monitoring data together and look for trends and attackers and organized threats that they can then protect our infrastructure against,” she explained. “It will take a while for them to get there, but imagine a repository that will maintain the threats and vulnerabilities that come from potential attackers — one that contains information for law enforcement to be able to do something about it.” ●

GROWING CONCERN ABOUT CLOUD SECURITY

% of respondents who think cloud computing's security risks are greater than risks for on-premises systems

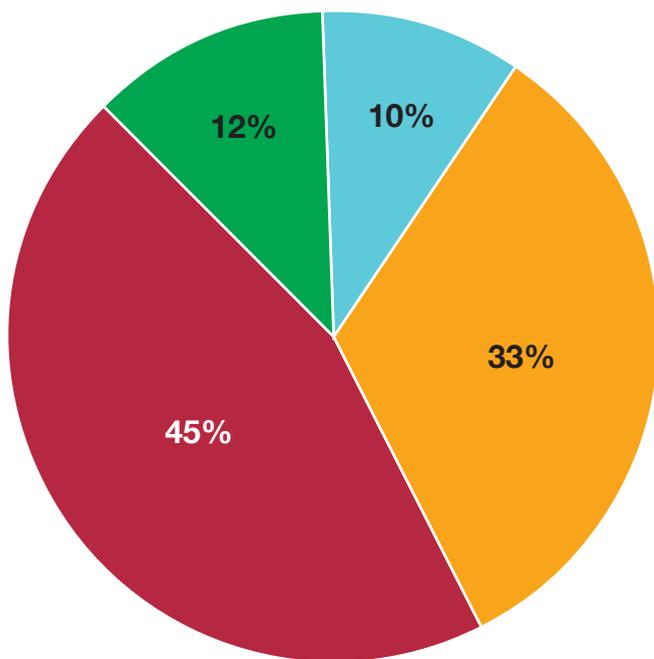


Lukewarm views of FedRAMP?

Nearly half of federal employees surveyed have no idea what the Federal Risk and Authorization Management Program is, much less the impact it will have on their agencies' IT applications and infrastructure. A January 2012 survey of almost 300 government IT officials, including nearly 200 federal government employees or contractors, by the 1105 Government Information Group found that only a quarter knew enough to have an opinion about the program.

FEDRAMP FAMILIARITY

% of respondents who are familiar with the FedRAMP guidelines for cloud security



- Know enough to form an opinion
- Know a little
- Very familiar
- Not aware

FedRAMP was developed by the CIO Council to establish a consistent approach to security for cloud computing across the federal government. It was signed into policy in December 2011 after more than a year of discussion.

Even though agencies eventually will have to comply with its security requirements, more than half have no opinion about whether it will achieve its stated goals: lowering

operational costs, saving time during cloud vendor selection, accelerating adoption of the cloud, promoting stronger interagency cooperation, being robust enough to guarantee security in the cloud, and improving continuous monitoring practices within agencies and departments.

Of those surveyed who do have strong opinions, 28 percent believe that FedRAMP won't have sufficient security, won't address new security threats, and will put up roadblocks in getting third-party cloud service providers certified. In fact, 29 percent responded that they don't expect that their agencies will use FedRAMP. The most common reason given was because of security concerns.

That's not surprising, said Kyra Kozemchak, a senior research analyst at Deltek, a Herndon, Va., government IT research and software development firm, because FedRAMP has had to accommodate a broad range of security concerns, standards and acceptable levels of risk across the federal government. FedRAMP was designed to address the basic security requirements applicable to all agencies, but if agencies are anticipating a higher level of security needs, it doesn't seem immediately applicable, she said.

"The FedRAMP group realizes that some agencies and departments need more security than FedRAMP provides, and there has been extensive dialogue between the FedRAMP office and defense organizations in particular about whether the baseline is high enough," she said. "Ultimately, where an agency's requirements exceed the minimum security identified by FedRAMP, service providers will need to meet that higher level."

Another reason for the lukewarm reception to FedRAMP probably has to do with human nature, said Kevin Jackson, general manager for cloud services at NJVC, a Vienna, Va., technology services provider for government. Jackson also is CIO of GovCloud.com, a site with cloud computing news that's relevant to the government market.

"It's a culture change. CIOs are now being told that their authority within the agency will be reduced because instead of them having control over the certification and accreditation process, 80 percent will be governed by FedRAMP," he explained.

Kozemchak contends that over time, perceptions will change. Those perceptions will be partly influenced by the FedRAMP group working out some kinks but mostly by federal users getting used to the idea and beginning to actually implement cloud using FedRAMP specifications.

There is still a long road ahead. Applications for authority to operate will be accepted starting in June. It will take the rest of 2012 for cloud service providers to go through



certification and for initial operations to get underway, and it will take yet another year to execute full operational capabilities. In the meantime, agencies with existing cloud services and authority to operate will have more than two years before they would have to be fully compliant.

“That means almost three years could pass from the FedRAMP policy memorandum release last year before an agency migrates its services,” Kozemchak said. “There is a lot of time that has to pass before agencies will really see if it’s a success, and by that time, a lot of the concerns may have faded.” ●



THE DATA CENTER IS HERE

Brocade is helping federal agencies deliver data center-class reliability and scalability to the edges of the network and into the cloud.

Brocade. Unlock the full potential of the cloud.

Brocade is, quite simply, the leader in cloud-optimized networking for the federal government. With the largest breadth of federally certified products, Brocade is committed to achieving the highest standards of interoperability and reliability required for all federal solutions and the Cloud First mandate. Brocade builds network foundations that ensure federal data center consolidations enable cutting-edge cloud services, seamlessly.

When the mission is critical, the network is Brocade.



BROCADE